

# INTEGRACIÓN DE LA ESTRATEGIA DE PROTECCIÓN DE ACTIVOS DE INFORMACIÓN AL PLAN DE RECUPERACIÓN DE DESASTRES DE UNA CASA DE SOFTWARE BAJO LA NORMA GTC-ISO/TS 22317:2015 (mayo de 2020)

Wilson Castillo Torres., Alfonso Luque Romero.  
[wilcasttor@gmail.com](mailto:wilcasttor@gmail.com) , [aluque18@ucatolica.edu.co](mailto:aluque18@ucatolica.edu.co)

**Resumen** – Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades, las cuales están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas.

Para el desarrollo de lo anterior se propone en este estudio una identificación de los activos de la fábrica de software como parte de la implementación de un análisis de impacto del negocio de la norma GTC-ISO/TS 22317 con el fin de determinar la importancia de estos a través de la clasificación y reconocimiento del valor intangible de componentes de desarrollo, piezas de código, artefactos y entregables con el fin de realizar un estudio del riesgo como factor desequilibrante de la estabilidad de la operación y facilitar una serie de recomendaciones que puedan aplicarse para generar un plan de recuperación de desastres adecuado.

**Índice de Términos:** Análisis de riesgos, GTC-ISO/TS 22317, Priorización de procesos, Valoración de activos.

**Abstract:** Information risks are present when two elements come together: threats and vulnerabilities, these are intimately linked, and there can be no consequences without their joint presence.

For the development of the above, this study proposes an identification of the assets of the software factory as part of the implementation of a business impact analysis of the GTC-ISO/TS 22317 standard in order to determine the importance of these through the classification and recognition of the intangible value of development components, pieces of code, artifacts and deliverables in order to carry out a study of the risk as a factor unbalancing the stability of the operation and to provide a series of recommendations that can be applied to generate an appropriate disaster recovery plan.

**Index of Terms:** Risk Analysis, GTC-ISO/TS 22317, Process Prioritization, Asset Valuation.

## I. INTRODUCCIÓN

Dentro del aseguramiento de la información hay que tomar en cuenta a la misma como un activo más en la organización, donde su alteración o pérdida puede acarrear efectos económicos y reputacionales que puede acabar con el ‘good will’ de toda empresa, dentro del plan para proteger la operación de todo negocio existe el plan de recuperación de desastres como alternativa de protección de la información basándose en el valor real que esta tenga para las operaciones y en coherencia con el apetito de riesgo en la organización frente a incidentes en los que sus datos se encuentren involucrados.

Hoy día, la información no se protege y preserva sólo para que no sea dañada, sino por la importancia y el uso que ésta tiene en todos los ámbitos de la vida. El comercio internacional, las instituciones bancarias y todo tipo de empresas mantienen sus operaciones gracias a que la información fluye a través de todos sus departamentos y áreas. La información se utiliza en cualquier empresa para realizar cuatro tipos de actividades: planeación, dirección, organización y control, las cuales fueron definidas hace más de 100 años por el ingeniero francés Henry Fayol. Lo que significa que la información se preserva para llevar a cabo en forma óptima el proceso administrativo dentro de cualquier organización, de cualquier tipo de actividad y cualquier tamaño. [1]

En una fábrica de software es muy frecuente el uso y desarrollo de piezas de información encaminadas a la producción de productos y servicios de Software que merecen toda protección en cuanto a su confidencialidad, integridad y disponibilidad dentro de los procesos de análisis, diseño, construcción e implementación de proyectos. Cada uno de los artefactos que se producen en este proceso se constituyen como activos de información que poseen propiedad material e intelectual y redundan en capital intangible de todo negocio de creación y gestión de programas informáticos.

Según datos de Fedesoft, la industria del software en Colombia agrupa a 6.096 empresas que facturan 13,5 billones de pesos al año, creció a una tasa anual promedio extraordinaria del 16,7 por ciento durante los últimos 6 años y representa un 1,6 por ciento del PIB. Estas empresas, que en un 90 por ciento son micro y pequeñas y en un 40 por ciento tienen cinco o menos años de vida, emplean 109.000 personas; y el gremio calcula que el sector presenta 45.000 vacantes. No existe una industria con mayor capacidad de ofrecer oportunidades de trabajo de calidad para el largo plazo, y a su vez, con mayor potencial de inclusión. En el mundo del software poco pesan las palancas y los títulos; prima la capacidad para programar. [2]

A nivel profesional, las organizaciones, sin importar su naturaleza, al igual que las personas, dependen de alguna manera de la tecnología de la información como una herramienta esencial para lograr sus objetivos de negocio o para poder desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy.

## II. MÉTODOS E INSTRUMENTOS

### A. Fases del Trabajo de Grado

El proyecto se ha estructurado en 4 fases para el cumplimiento de los objetivos las cuales son:

**Fase 1: Levantamiento de información:** En esta fase se realizará el contacto inicial con las áreas sometidas a estudio, realizando análisis de la estructura de la organización e identificación de los procesos documentados en la entidad.

**Fase 2: Análisis y organización del levantamiento:** Usando como instrumento una encuesta la cual será estructurada para ello y aplicada al área de estrategia y arquitectura, posteriormente se analizarán los resultados y se levantará una identificación de activos de información, se contrastará contra documentos que estén relacionados con el plan de continuidad y se realizará un análisis de la estrategia de adaptación del marco metodológico basado en la elaboración de la cascada de metas propia del marco de referencia COBIT v5, con el fin de comprobar la prioridad de procesos asociados a continuidad de negocio y gestión de activos.

**Fase 3: Diagnóstico y planteamiento de estrategia de protección:** En esta fase se realizará la clasificación de los activos identificados que permitan su valoración conforme a la Guía 5 de MinTIC y la evaluación de riesgos asociados a los mismos.

**Fase 4: Generación de propuesta y comunicación de los resultados:** En esta fase se realizará la generación de recomendaciones encaminado a la elaboración de un posible plan de recuperación de desastres tomando como referencia la norma GTC/ISO 22317, realizando la entrega y la comunicación de la estrategia planteada.

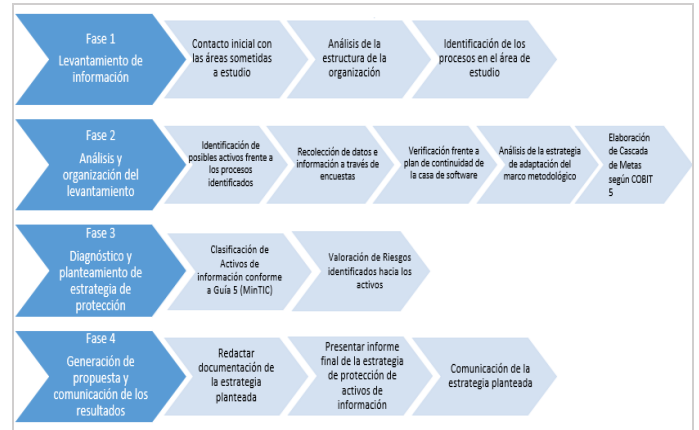


Fig. 1. Fases del proyecto de grado

### B. Desarrollo de la propuesta

Para llevar a cabo los objetivos establecidos, en el proyecto se tomará en cuenta una adaptación de los propuesto en la Guía Técnica Colombiana GTC-ISO/TS 22317 'Seguridad de la sociedad. Sistemas de Gestión de la Continuidad del Negocio. Directrices para el Análisis del Impacto del Negocio' y de lo especificado por la 'Guía para la gestión y clasificación de activos de información' de MinTIC.

- **Información de los activos de información:** se debe realiza levantamiento de información relacionada con la entidad a la cual se tiene como objetivo del proyecto es aquí donde se debe levantar información de procesos subprocesos descripción de los mismos y un contexto externo e interno de la organización sobre la cual se realizará lo propuesto.
- **Definición:** Se realizará la definición de los activos de información donde se pueda percibir una concordancia frente a los procesos del negocio y la familiarización realizada en el área.

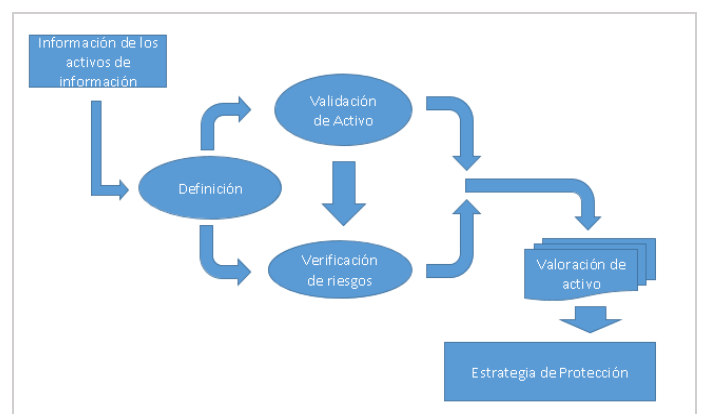


Fig. 2. Fases del proyecto de grado

### C. Instrumentos o Herramientas utilizadas

Para el desarrollo del presente proyecto se van a utilizar los siguientes instrumentos o herramientas:

- Encuestas (formularios de google)

- COBIT v5 “Proceso catalizadores\_ Cascada de Metas”.
- Guía Técnica Colombiana (GTC-ISO/TS 22317)
- Material de procesos y procedimientos del área de tecnología (a los cuales se tenga acceso)
- Guía 5 MinTIC “Guía para la gestión y clasificación de activos de información”.
- Herramientas de ofimática

### III. RESULTADOS Y DISCUSIÓN

Como resultado se plantea definir los activos de alto valor para la organización, estableciendo los riesgos a los cuales pueden verse asociados los activos.

#### A. Resultados esperados Fase 1

Siendo consistentes con la norma GTC- ISO/TS 22317 el éxito de los resultados de un proceso BIA depende de que la organización entienda:

- El ambiente externo en el que opera, de manera que pueda lograr su propósito mediante la entrega de sus productos y servicios a sus clientes;
- El ambiente operativo interno, incluidos los procesos actividades y recursos, así como el impacto potencial causado por la interrupción en la entrega de productos y servicios y
- Las leyes y reglamentos que gobiernan el proceso BIA y la manera como se realiza [3]

Se realizó un análisis de la estructura de la organización de acuerdo a la información compendiada, definiendo la historia de la Casa de Software y analizando los procesos que constituyen los objetivos del negocio encontrando que procesos como Servicio al cliente, Gestión de recursos físicos, Planeación estratégica, Venta consultiva, Transición de la solución e Infraestructura tecnológica No se encuentran documentados razón por la cual no se definen activos de información desde la documentación del proceso.

Con el objetivo de realizar la definición de los activos de información, se hace necesario determinar cuáles son los procesos que se encuentran involucrados dentro de la casa de software y los elementos que interactúan entre ellos, lo anterior con el fin de determinar posibles activos que se encuentren citados en el establecimiento de estos.

Por tal razón, se procede a analizar los procesos que se encuentran constituidos para la Casa de Software, en donde se tendrá en cuenta el establecimiento de cada uno de los mismos la mención a supuestos activos que tengan relación, esto debe contemplar repositorios de información, documentación extraída, sitios de almacenamiento de código, productos generados y componentes de infraestructura.

A continuación, se relacionan los procesos encontrados una breve descripción de cada proceso posibles responsables y los activos de información que hayan sido detectados en la lectura de estos:

Tabla 1. Tabla de procesos

Proceso	Descripción
Arquitectura	Encargado de analizar las posibles alternativas una decisión a tomar utilizar un proceso formal que dichas alternativas identificadas frente a criterios establecidos para tomar la mejor decisión.
Aseguramiento de la calidad de los procesos	Proporciona al personal y a la gerencia una visión objetiva de los procesos a través de la identificación de no conformidades y asegurando la resolución de las mismas.
Control de calidad productos y servicios	Este proceso se encarga de verificar y validar que los productos y servicios de la organización sean liberados con un alto índice de calidad logrando la satisfacción de nuestros clientes.
Diseño, desarrollo Integración y despliegue	Este proceso tiene como propósito diseñar, desarrollar e integrar y desplegar una solución de software con altos estándares de calidad.
Entrenamiento Organizacional	Este proceso se encarga de gestionar coordinadamente todas las necesidades y esfuerzos de capacitación que requieran los colaboradores a fin de desarrollar las habilidades necesarias para la ejecución efectiva de sus actividades.
Gestión de la Configuración	Este proceso tiene como principal objetivo planear Identificar y mantener la integridad en la administración de los ítems de configuración (productos de trabajo de la empresa) tratando líneas base que permitan a la empresa tener puntos de referencias para mantener la coherencia y calidad en los proyectos que se desarrollan.
Gestión de procesos	Este proceso establece y mantiene un conjunto estable de activos de procesos de la organización y estándares del entorno del trabajo, además; planifica, implementa y despliegan las mejoras a dichos procesos.
Gestión de proyectos	Este proceso de escribir aplicación de conocimientos habilidades, herramientas y técnicas de las actividades de los proyectos de tal forma que se cumplan con los requerimientos establecidos dentro de cada proyecto. Esta sección incluye el inicio, planeación, ejecución, monitoreo, control y cierre de un proyecto.
Gestión de recursos físicos	No posee Información
Gestión del portafolio de Proyectos	Este proceso permite centralizar y coordinar la dirección de proyectos a cargo del grupo de gerentes de proyectos y garantizar el cumplimiento de los mismos.
Ingeniería de Requisitos	Este proceso permite identificar analizar documentar y diseñar y entregar los requerimientos del producto a partir de las necesidades del cliente .
Medición y análisis	Este proceso tiene como propósito implementar una metodología que permita asegurar que los objetivos y las actividades de medición y análisis estén alineados con las necesidades de información y objetivos identificados por la dirección mediante la creación uso y modificación de métricas.
Planeación estratégica	No posee información
Servicio al cliente	No posee información
Toma de decisiones formales	Este proceso se encarga de analizar las posibles alternativas a una decisión a tomar utilizando un proceso formal que evalúe dichas alternativas identificadas frente a criterios establecidos para tomar la mejor decisión
Venta Consultiva	No posee información
Transición de la solución	No posee información
Infraestructura tecnológica	No posee información

#### B. Resultados esperados Fase 2

Se procede a comparar los procesos reportados por el plan de Continuidad con los procesos publicados por la entidad, ya que estos fueron usados para el levantamiento de información desarrollo de la entrevista de campo, por tal motivo se procede a levantar el contraste con los procesos definidos como críticos por el plan de continuidad y los procesos similares que se encuentren publicados y definir los procesos a trabajar en el desarrollo del presente documento:

Tabla 2. Contraste Procesos publicados y Procesos en Plan de Continuidad

Proceso validado	Proceso Publicado	Proceso definido en Plan de continuidad como críticos	Observación
Servicio al cliente	Servicio al cliente	Soporte a Clientes (2do y 3er Nivel) - Mesa de Servicio	Se debe definir el proceso para validar la concordancia con lo definido en el plan de continuidad
Desarrollo	Diseño, desarrollo, integración y despliegue	Desarrollo de aplicaciones	Se recomienda definir el desarrollo dentro
Aseguramiento de la calidad	Control de calidad productos y servicios	Aseguramiento de la calidad	Se debe definir si se hace referencia al control de calidad de los productos y servicios o al aseguramiento de la calidad de los procesos
Despliegue	Diseño, desarrollo, integración y despliegue	Entrega de desarrollo a clientes	Se recomienda definir la entrega de desarrollo como parte del proceso de 'Diseño, desarrollo, integración y despliegue'

- Adaptación de Cascada de metas de COBIT para priorización de procesos

De acuerdo con la norma GTC-ISO/TS 22317 el proceso BIA prioriza los diferentes componentes organizacionales de manera que la entrega de productos y servicios se pueda reanudar en un periodo de tiempo predeterminado luego de un incidente de interrupción para la satisfacción de las partes interesadas. Para los propósitos del presente documento y de coherencia con la NTC 5722 (ISO 22301) los productos y servicios son creados por procesos que a su vez están compuestos de actividades.

Los productos y servicios se priorizan primero; así se establecen los parámetros de tiempo y nivel de servicio para la priorización de procesos. Si así lo exige la complejidad de la organización los procesos se pueden separar en sus actividades componentes para llevar a cabo la priorización. [4]

Considerando el tiempo de ejecución del proyecto, se decide adaptar el uso de la cascada de metas de COBIT v5 para el desarrollo de la priorización de los procesos tomando en cuenta el éxito de dicha cascada al momento de generar la priorización de habilitadores en procesos organizacionales, con esta se espera suplir parte de las necesidades que puede ejecutar un análisis de impacto del negocio. (BIA), tomando en cuenta que los procesos críticos a evaluar corresponden a los procesos mínimos de operación con los que puede operar la casa de software, se hace viable el uso de la cascada de metas de COBIT v5 para obtener los procesos habilitadores que refuercen el desarrollo de la estrategia de protección aplicable a la organización.

Para el estudio, se debe comprender que cada negocio, como la casa de software, se comprende de forma distinta y la organización puede determinar objetivos y funciones misionales conforme a su realidad actual y a sus objetivos de mercado; cuyo contexto es determinado por factores externos e internos que resaltan al momento de considerar un sistema de gobierno y gestión a la medida. donde los interesados y sus necesidades se convierten en estrategias corporativas factibles para el desarrollo del modelo de negocio.

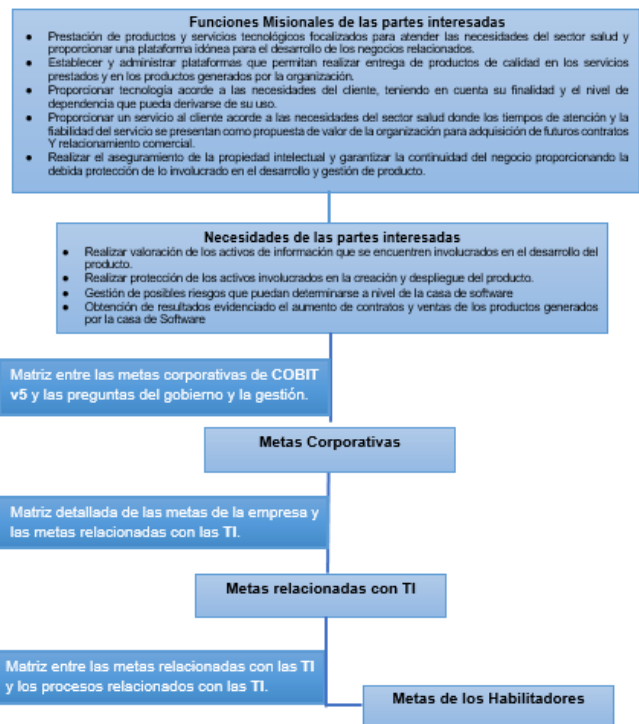


Fig. 3. Cascada de metas Casa de Software.

- Totalización procesos habilitadores relacionados con procesos críticos

Al realizar la cascada de metas propuesta por COBIT v5 se logró priorizar los procesos como habilitadores que deben ser tenidos en cuenta en el planteamiento de la estrategia dirigida a la concepción de un plan de recuperación de desastres donde se demuestra que la organización prioriza la gestión de la continuidad dentro de los habilitadores importantes dentro de la estrategia, de igual forma se evidencia la conciencia relacionada con la gestión de los activos involucrados; el instrumento de la cascada de metas permite elaborar una descripción de los procesos que deben ser tenidos en cuenta al momento de plantear una estrategia de protección, razón por la cual y siendo consistentes con la norma GTC-ISO/TS 22317, ya que permite identificar productos y servicios que deben ser gestionados desde la estrategia ofreciendo una herramienta base para determinar las categorías y criterios de impactos.

Tabla 3. Totalización habilitadores críticos necesarios para la generación de la estrategia

		PUNTAJES			PUNTAJE	TOTAL
		CAJADA	VALOR 1	VALOR 2		
Asigne un Peso a cada Criterio de Calificación:			3	2	1	
PROCESOS COBIT 5			VALOR 1	VALOR 2	VALOR 3	
Evaluar, Orientar y Supervisar	EDM02	Asegurar la entrega de beneficios	5	3	3	24
	EDM04	Asegurar la optimización de recursos	4	4	5	25
	APD01	Gestionar el marco de gestión de TI	5	3	5	26
Alinear, Planificar y Organizar	APD02	Gestionar la estrategia	5	5	4	29
	APD05	Gestionar el portafolio	4	4	5	25
	BAI08	Gestionar el conocimiento	3	1	5	16
Construcción, Adquisición e Implementación	BAI09	Gestionar los activos	2	1	5	13
	BAI10	Gestionar la configuración	3	1	3	14
	DSS04	Gestionar la continuidad	5	2	5	24

Fuente: Matriz tomada de COBIT v5 Framework – Formulación adaptada de documento FERROL INTERNATIONAL GROUP

### C. Resultados esperados Fase 3

De acuerdo con la norma GTC-ISO/TS 22317 el siguiente diagrama explica el proceso BIA, junto con los prerequisites y su relación con la identificación de estrategias [5]:

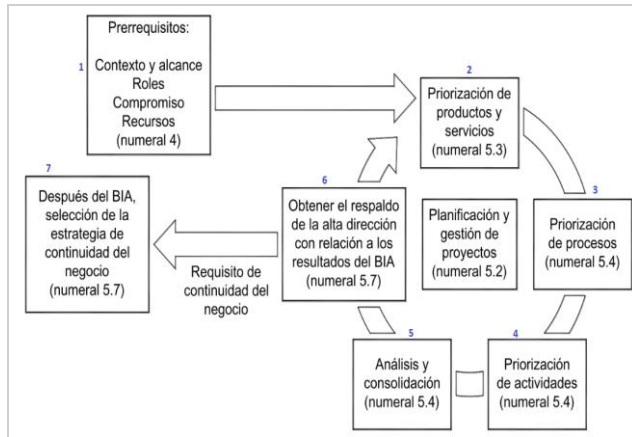


Fig. 4. Proceso de análisis de impacto en el negocio

Para la elaboración de esta fase en el presente proyecto se tuvieron en cuenta los siguientes estados del proceso de análisis de impacto en el negocio indicado por la norma GTC – ISO/TS 22317:

- Estado 2 (Priorización de productos y servicios)
- Estado 3 (Priorización de procesos)
- Estado 4 (Priorización de actividades)
- Estado 5 (Análisis y consolidación)

Con relación al estado 6 (Obtener el respaldo de la alta dirección con relación a los resultados del BIA), este fue consensado con la organización para desarrollarlo a través de la priorización de procesos, lo anterior con el fin de presentar información suficiente para la selección de la estrategia de continuidad del negocio. Con el fin de reforzar la información de la estrategia seleccionada se debe desarrollar el análisis de impacto en el negocio, el cual no será desarrollado en este proyecto

- Clasificación de Activos de información con mayor relevancia para la elaboración de la estrategia conforme a Guía 5 (MinTIC)

Al identificar los activos de cada proceso se puede determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, unos archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios). Así la Casa de Software puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento externo, aumentando así su confianza en el uso del entorno digital [6]

Tabla 4. Muestra de Activos con Clasificación Alta

Código	Proceso	Recurso	Activo	Tipo Activo	Descripción	Confidencialidad	Integridad	Disponibilidad	Valor Corporativo	Valor Final Estimado
ACT2	Control de calidad productos y servicios	Repositorio de trazabilidad	Versión de código	Información	Repositorio donde se almacena las versiones del desarrollo y piezas de código.	2	3	3	3	3
ACT10	Diseño, desarrollo Integración y despliegue	Repositorio de Trazabilidad	Versión de código	Sistema de Información	Repositorio donde se almacena las versiones del desarrollo y piezas de código.	3	3	3	3	3
ACT12	Diseño, desarrollo Integración y despliegue	Línea base producto para despliegue	Versión de código	Información	Repositorio donde se almacena las versiones del desarrollo y piezas de código que han sido definidas para integración y despliegue de la solución producto.	3	3	2	3	3

Al realizar la **valoración de activos** conforme a lo especificado por la guía de clasificación de información #5 de MinTIC se logró presentar una forma estándar para comprender la importancia de la información para la organización, coadyuvando al cumplimiento de la priorización de productos y servicios, principalmente, con el aseguramiento de la continuidad de la misma, siendo consistente con lo especificado por la Norma GTC-ISO/TS 22317, el caso aplicado toma como base la determinación de activos dirigidos a los objetivos del negocio.

- Resultado de Valoración de Riesgos identificados hacia los activos con nivel de riesgo alto y extremo

La evaluación del riesgo permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de una organización; de esta forma es posible distinguir entre los riesgos Bajos, Moderados, Medios, Altos y Extremos y fijar las prioridades de las acciones requeridas para su tratamiento.

Para facilitar la calificación y evaluación a los riesgos, se generó la tabla presentada anteriormente donde se contempla un análisis cualitativo realizado en conjunto con la entidad, para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad). [7]

Tabla 5. Muestra de Valoración de riesgos identificados hacia los activos con nivel de riesgo alto y extremo

Valor probabilidad	Nivel probabilidad	Valor impacto	Nivel impacto	Valor Rango	Nivel Riesgo
5	Casi seguro	5	Extremo	5	Extremo
4	Probable	4	Alto	4	Alto
3	Posible	3	Medio	3	Medio
2	Improbable	2	Moderado	2	Moderado
1	Raro	1	Bajo	1	Bajo

Código Riesgo	Nombre del Activo	Descripción Activo	Tipo Activo	Área	Vulnerabilidad	Reducción del Riesgo	Probabilidad de Ocurrencia	Impacto					Puntaje Total	Nivel de Riesgo
								Reputacional	Información	Operativa	Financiera	Legal		
ACT1	Información almacenada en plataforma centralizada	Repositorio de consulta y actualización de documentos donde se almacena la documentación enviada por desarrollo para realizar procesos de pruebas al producto, de igual forma también se encuentra el código de funcionamiento del desarrollo a probar.	Base de datos	Desarrollo	Almacenamiento sin protección	Posible daño del hardware de almacenamiento por hardware, debido a la falta de mantenimiento del área de almacenamiento, afectando la integridad, disponibilidad y oportunidad de la información almacenada.	3	3	4	3	4	4	4	Alto
ACT1	Información almacenada en plataforma centralizada	Repositorio de consulta y actualización de documentos donde se almacena la documentación enviada por desarrollo para realizar procesos de pruebas al producto, de igual forma también se encuentra el código de funcionamiento del desarrollo a probar.	Base de datos	Desarrollo	Accesibilidad a los datos del equipo	Posible daño del servidor con misión crítica por caída constante de Node.js debido a la falta de mantenimiento de la información y la disponibilidad de los equipos.	2	3	4	3	4	4	4	Alto



#### D. Resultados esperados Fase 4

De acuerdo con la norma GTC-ISO/TS 22317 para cada grupo de productos y servicios, la alta dirección debería decidir y documentar lo siguiente:

- El tiempo después del cual la falla en la entrega de productos o servicios se convierte en inaceptable para la organización debido a que los impactos ya mencionados amenazan su supervivencia o hacen que ya no pueda cumplir sus objetivos.
- Las razones por las cuales se ha identificado este período de tiempo con referencia a los impactos crecientes a lo largo del tiempo [8]

Una opción de tratamiento definida por la norma es realizar un planetamiento basado en escenarios.

El escenario de desastre es la representación de la interacción de los diferentes factores de riesgo (peligro y la vulnerabilidad), en un territorio y en un momento dado. Significa una consideración pormenorizada de las amenazas (peligros) y vulnerabilidades y, como metodología, ofrece una base para la toma de decisiones sobre la intervención en reducción, revisión y control de riesgo. [9]

Se realiza planteamiento de estrategia de protección como insumo para la generación de un plan de recuperación de desastres (DRP) tomando en cuenta la necesidad de continuidad dentro de la priorización de sus procesos.

Se realiza generación de la propuesta tomando en cuenta los siguientes componentes de la estrategia:

Tabla 6. Componentes de planteamiento de estrategia

Componente Estrategia	Descripción	Ubicación en el Documento
Escenarios de desastre	Escenarios simulados propuesto que iniciaran labores de recuperación de desastres.	<a href="#">5.4.1 Escenarios de desastre</a>
Información de procesos críticos con RTO Y RPO	Información de procesos donde se definen puntos y tiempos objetivos de recuperación (RPO y RTO) para los procesos en estudio.	<a href="#">5.4.2 Información de procesos críticos con RTO Y RPO</a>
Información de recursos necesarios en la estrategia de protección	Información de procesos donde se definen puntos y tiempos objetivos de recuperación (RPO y RTO) para los procesos en estudio	<a href="#">5.4.3 Información de recursos necesarios en la estrategia de protección</a>
Operación Alterna en caso de contingencia	Define la estrategia general de operación alterna	<a href="#">5.4.4 Operación Alterna en caso de contingencia</a>
Clientes en Operación Mínima en caso de contingencia	Define la configuración mínima de los clientes que se encuentran en operación alterna	<a href="#">5.5.5 Clientes en Operación Mínima en caso de contingencia</a>
Procedimientos antes del incidente	Describe las actividades a considerar antes de la ocurrencia de un incidente	<a href="#">5.4.6 Procedimientos antes del incidente</a>
Procedimientos durante el incidente	Describe las actividades a considerar durante la ocurrencia de un incidente y su correspondiente activación de contingencia	<a href="#">5.4.7 Procedimientos durante el incidente</a>
Procedimientos después del incidente	Describe las actividades a considerar después de contingencia y eventos para retornar a la operación	<a href="#">5.4.8 Procedimientos después del incidente</a>
Proveedores Operación Crítica	Describe los proveedores descritos que deben apoyar labores de contingencia y eventos para retornar a la operación	<a href="#">5.4.9 Proveedores Operación Crítica</a>
Personas Operación Crítica	Describe las personas mínimas requeridas que deben apoyar labores de contingencia y eventos para retornar a la operación	<a href="#">5.4.10 Personas Operación Crítica</a>

#### IV. CONCLUSIONES

- Adaptar la cascada de metas de COBIT v5 sirve como herramienta de contraste para realizar priorización de procesos previamente constituidos, si bien es cierto que no reemplaza la implementación de un análisis de impacto del negocio si sirve para establecer la base para una generación de una estrategia de protección de activos de información

- Con el análisis de riesgos, se logró verificar la importancia del activo teniendo en cuenta las amenazas y vulnerabilidades a las que está expuesto, de igual forma estimar la importancia de lo mínimo con que debe contra la estrategia de protección para proteger los activos contemplados en los procesos.

- Con la clasificación de activos de información se logró brindar un nivel de tratamiento a cada tipo de activo, esto con el fin de proteger su integridad, confidencialidad y disponibilidad, además de usar guías propuestas por el gobierno de Colombia que sirvan para constatar la preservación de activos intangibles en organizaciones de diversa naturaleza

- La estrategia de protección definida en un plan de recuperación de desastres (DRP) permite que la organización logre definir componentes que puedan estar involucrados desde una posición holística a la tecnología y encausar la importancia de sus equipos, herramientas e información para dar un tratamiento adecuado y constituirlo como parte integral de un esquema de continuidad del Negocio.

#### RECONOCIMIENTO

Agradecimiento del autor al asesor de proyecto, el Ing. Alfonso Luque Romero, por su visión, apoyo y disposición para la elaboración de esta investigación y al Ing. Jhon Fredy Cardona por sus recomendaciones y el apoyo a un miembro de su equipo en apuros.

#### REFERENCES

- [ 1 ] G. Baca Urbina, de Introducción a la seguridad informática, Mexico, Grupo Editorial Patria, 2016, p. XIII.
- [ 2 ] Revista Semana, «La clave es el “software”», 17 10 2018. [En línea]. Available: <https://www.semana.com/opinion/articulo/industria-del-software-en-colombia-columna-de-esteban-piedrahita/587171>. [Último acceso: 26 03 2020].
- [ 3 ] Icontec, «Guía Técnica Colombiana GTC- ISO/TS 22317,» de Seguridad de la Sociedad. Sistemas de Gestión de la Continuidad de Negocio \_ Directrices para el Análisis de Impacto en el Negocio (BIA), Bogotá, Icontec, 2012, p. 6.
- [ 4 ] Icontec, «Guía Técnica Colombiana GTC- ISO/TS 22317,» de Seguridad de la Sociedad. Sistemas de Gestión de la Continuidad de Negocio \_ Directrices para el Análisis de Impacto en el Negocio (BIA), Bogotá, Icontec, 2012, p. 6.

- [ 5 ] Icontec, «Guía Técnica Colombiana GTC- ISO/TS 22317,» de Seguridad de la Sociedad. Sistemas de Gestión de la Continuidad de Negocio \_ Directrices para el Análisis de Impacto en el Negocio (BIA), Bogotá, Icontec, 2012, p. iii.
- [ 6 ] Departamento Administrativo de la función pública (DAFP), «Guía para administración del riesgo y el diseño de controles en entidades públicas,» DAFP, 10 2018. [En línea]. Available: [www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%ABlicas+-+Riesgos+de+gesti%C3%B3n%2C+corrupci%C3%B3n+y+seguridad+digital+-+Versi%C3%B3n+4+-+Octubre+de+20](http://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%ABlicas+-+Riesgos+de+gesti%C3%B3n%2C+corrupci%C3%B3n+y+seguridad+digital+-+Versi%C3%B3n+4+-+Octubre+de+20). [Último acceso: 06 05 2020].
- [ 7 ] Departamento Administrativo de la función pública (DAFP), «Guía para administración del riesgo,» DAFP, 09 2011. [En línea]. Available: <https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba>. [Último acceso: 06 05 2020].
- [ 8 ] Icontec, «Guía Técnica Colombiana GTC- ISO/TS 22317,» de Seguridad de la Sociedad. Sistemas de Gestión de la Continuidad de Negocio \_ Directrices para el Análisis de Impacto en el Negocio (BIA), Bogotá, Icontec, 2012, p. 10.
- [ 9 ] Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres (CENEPRED), «Escenario de riesgos,» CENEPRED, 01 2019. [En línea]. Available: <https://www.indeci.gob.pe/wp-content/uploads/2019/01/fil20160516082630.pdf> . [Último acceso: 06 05 2020].



**Alfonso Luque Romero**

Ingeniero de Sistemas, Magister en Sistemas de Información, se ha desempeñado como Auditor de TI, Jefe Operativo y Delegado de Auditoría Industrial en el Banco de la República de Colombia. Auditor Certificado – CISA, CISM y COBIT Foundations. Experiencia en Planeación y Ejecución de Auditorías de Sistemas, Auditorías Operativas y Financieras y en la Implementación de Sistemas de Administración de Riesgo Operativo. Ha participado como conferencista y docente a nivel local y latinoamericano en temas de Auditoría de Sistemas, Seguridad Informática y Tecnologías de la Información.

## Biografía Autores



**Wilson Castillo Torres**

Ingeniero en Telemática

Universidad Distrital Francisco José de Caldas

Especialista en Auditoria de Sistemas de Información

Universidad Católica de Colombia